I. INTRODUCTION

The U.S. has an established record of exploiting crisis decision-making to justify heightened levels of policing and surveillance. From Japanese American internment camps during WWII, to the “Special Registration” of Arabs, South Asians, and Muslims after 9/11, authorities have repeatedly extended and misused emergency powers to criminalize Black, Brown, and immigrant communities.

As the U.S. grapples with the COVID-19 pandemic, we work together with our neighbors, our employers, and our government to mitigate the immediate public health danger to our communities. New policies, laws and announcements emerge daily which make it far easier for government and private companies to collect and share vast amounts of our personal and private health information. While this data may be critically important from a public health function, there are many unknowns around its future use.

Many tech corporations, such as Palantir, already sell massive data collection and data and analytics services to government agencies, including police departments and Immigration and Customs Enforcement. Now, with the support of this administration, they are building systems for U.S. health care agencies.¹
History tells us that laws, practices, and data persist long after an initial emergency subsides.

Governments and companies will seek to re-purpose emergency surveillance and practices to carry out other political agendas such as deportation and criminalization of immigrants and Black and Brown people. An emergency practice, once seen as an extraordinary and temporary crisis measure, becomes the new norm.

This advisory will (1) summarize health surveillance policy, (2) outline 5 ways in which government agencies and corporations are using advanced technologies to conduct more intrusive surveillance, and (3) offer general recommendations for our communities as we endure this pandemic.

II. BACKGROUND ON HEALTH SURVEILLANCE

Health surveillance is a long-accepted practice in the medical community.² Typically, this surveillance means patient outcomes are regularly monitored and studied to determine the best way to tackle a medical problem, like cancer, diabetes, vaping or opioid addiction treatment. The Health and Human Services Agency and the Centers for Disease Control and Prevention (CDC) coordinate with state and city health care systems to conduct health surveillance and manage outbreaks.³ The CDC’s mandate and its accompanying surveillance program is vast—covering everything from cancer to bioterrorism. The CDC holds police powers, including over Customs and Border Protection (CBP), to manage an outbreak⁴ and is involved in immigration processing of refugees and immigrants.⁵

Sources of Big Data in Health Care. Source: IMS Institute for Healthcare Informatics
Moreover, the CDC’s inaugural surveillance “innovation plan” involves coordinating ongoing health surveillance and data sharing among corporations, health providers, and government agencies on U.S. populations, not just field investigations on particular diseases, like obesity or malaria.6

_In the stimulus package signed by President Trump last month, Congress provided $500 million for the CDC to create a new, massive “surveillance and data collection system” to track the spread of the coronavirus._

The CDC is required to give updates on this new data collection system every 30 days. House Speaker Pelosi recently created a new committee, House Select Committee on the Coronavirus Crisis, to monitor the implementation of new stimulus packages.7 Moreover, Congress created a Pandemic Response Accountability Committee (PRAC), composed of numerous Inspector Generals, through another stimulus package to oversee waste and fraud.

Congress did not specifically limit the level of surveillance nor did it limit the role of Silicon Valley and consulting companies on the collection and sharing of personal information. Everything from artificial intelligence analytics to GPS tracking and social media mining is on the table for surveillance beyond hospitals, including our neighborhoods and businesses.8 The White House and Congress have turned to Silicon Valley corporations, like Google and Facebook, many of whom own or collect massive amounts of personal data, to build these new systems for the CDC.9 Some of these partnerships have shown signs of falling flat.10

Our privacy laws contain large emergency power exceptions, and concerns are rising that companies will likely share vast amounts of personal information with government and police agencies.11 Already, agencies are relaxing privacy protections.12 _Immigration status is not automatically considered personal or private information._13 Oversight and monitoring of the new CDC systems will be critical in the upcoming months.
III. FIVE WAYS THAT GOVERNMENTS AND COMPANIES ARE USING THE PUBLIC HEALTH CRISIS TO EXPAND SURVEILLANCE

Government agencies including DHS and private companies have been developing technologies to track the physical location, biometrics data, and online data of residents long before the COVID-19 pandemic. Now, amid a global health crisis, governments and private companies are using the moment to dramatically accelerate and normalize various forms of mass surveillance. Below, we break down five major tools of mass surveillance during the COVID-19 pandemic.

1. LOCATION TRACKING AND SHARING WITH GOVERNMENT

In the public health context, the justification for location tracking has been (1) to monitor social distancing and compliance with stay-at-home orders that carry criminal and immigration consequences and (2) in some instances, to conduct contact tracing of infected or potentially infected individuals. However, there is little to no oversight of the government’s location surveillance program: we do not know the duration of this surveillance and data sharing; whether there are limitations on data use, retention or disclosure; and which federal, state and local agencies have access to this information.

In the last few weeks, the location tracking for COVID-19 purposes has rapidly expanded in the U.S. Below, we focus on two primary ways that companies and governments have been tracking our location: cell phone location data and facial recognition.

A. Cell Phone Location Tracking

Since the 2000s, technology companies have been developing technologies to track people’s location through cell phones. The most common method of cell phone location collection is applications on smartphones—anything from games to weather apps to local news—which allow the maker of the app to track and collect the phone’s location. The companies that collect this data then turn around and sell it to cell phone surveillance companies who in turn sell the data
to businesses and governments. Prior to the COVID-19 outbreak, the Department of Homeland Security bought some of this location data, leading to significant public outcry.\textsuperscript{15}

\textit{Now, the CDC and various other state and local agencies have real-time access to this expansive, location-tracking surveillance tool.} Disturbingly, cell phone surveillance companies can share this location data with government agencies with pinpoint detail.\textsuperscript{16} While publicly available location maps have some level of anonymization\textsuperscript{17} (only show aggregate data at the county level), the actual information collected by these companies and shared with governments is in far greater detail.\textsuperscript{18}

For example, in one recent incident, a phone surveillance company saw that many individuals were congregating in Prospect Park, Brooklyn in contravention of the stay-at-home order and reported the information to the local police.\textsuperscript{19}

Though companies have claimed that they will not share username information associated with a phone location with the government, anonymization of location data is nearly impossible if the government can map a phone’s precise location, for example at a home or office, at any given time.\textsuperscript{20} In South Korea, similar sharing of location data has led to the public unmasking of people and their private lives including accusations of an extramarital affair.\textsuperscript{21}

\begin{figure}
\centering
\includegraphics[width=\textwidth]{cell_phone_location_data_new_york_city}
\caption{Cell phone location data in New York City gathered from surveillance companies.}
\end{figure}

\\textit{Source: New York Times.} \textsuperscript{22}
Currently, a group of cell phone surveillance companies are building an online portal to their location data which can be accessed by federal, state and local officials for the purpose of this epidemic response. The portal would allow federal and local agencies to closely track cell phone location data in up to 500 cities in the U.S.\textsuperscript{23}

However, there is little to no information on the duration of this data surveillance, limitations on data use, or restrictions on data retention; or the federal or local agencies having access to this portal.

Other recent examples of cell phone location tracking for COVID-19 include:

- Google has launched a public tool that allows the public to track people’s movements by country and by county in the U.S.\textsuperscript{24}

- In Britain, the National Health System is designing a smart phone app that would allow residents to opt-in to share their location data and be alerted if someone who tested positive for COVID-19 is near them or previously came into contact with them.\textsuperscript{25}

- In Taiwan, cell phone location data is used to create an “electronic fence” which alerts authorities when a quarantined person moves too far away from their home.\textsuperscript{26}

- In South Korea, authorities are publishing detailed time and location data of individuals suspected to have tested positive for the virus using phone location data.\textsuperscript{27}

- In Lombardy, Italy, authorities are analyzing location data transmitted by phones to determine how many people are obeying a government lockdown order and the typical distances they move every day.\textsuperscript{28}
B. Facial Recognition Tracking

Facial recognition technology allows a user the ability to identify a person from a digital image, like a face-scan, or a video frame. Combined with an expansive and more powerful camera surveillance network, it can be a forceful tool in tracking the location of individuals. Facial recognition is nothing new; for years, it has been a topic of huge debate over privacy concerns and consumer protection. Now amid this public health crisis, facial recognition companies are seeking to justify and expand their services. Companies are advertising customizable services to governments that track citizens who may be positive for the coronavirus in order to enforce quarantines and stay-at-home orders or to prohibit access to stores or public spaces.

For example, in Moscow, the government uses automated facial recognition technology in its expansive CCTV network to catalogue those who are leaving their homes amid quarantine restrictions.29

According to the Wall Street Journal, Clearview AI-- a U.S. company which sells facial recognition technology made from billions of photos scraped from social media and the web--is among the companies working or in discussions with federal or state agencies in the U.S. about using their technology to track people with COVID-19.30

Additionally, as we discuss below, companies are designing new surveillance devices that combine facial recognition, biometric and behavior analysis, and remote body temperature sensors.

Example of facial recognition and behavior detection cameras in London. Source: LIFARS.
2. BODY TEMPERATURE AND HEALTH TRACKING

Amidst a pandemic, health technology companies have significantly expanded their health surveillance data collection and advertised their technologies to the federal and local agencies.

One fast growing area of health surveillance is temperature or “fever-tracking” because it is one indicator for COVID-19. Temperature tracking can take place in two ways: (1) “smart” thermometers that are connected to the internet, allowing the company to collect the data when a person takes their temperature; and (2) remote temperature sensing devices.

“Smart” thermometers: In the past decade, companies like Kinsa have developed internet-connected thermometers which allow the company to collect and track the data. Often, information collected by these companies is not anonymized since it is specific to your thermometer and smart phone app. Currently, some of these companies are publicly sharing the data online though it is anonymized to the county-level.\(^{31}\)

Biometric detection technology is a fast-evolving industry. Recently, the company Oura developed a smart ring that could not only measure temperature but other vital signs when worn. In March, University of California San Francisco Medical Center had 2,000 emergency medical workers wear these rings to identify the early onset of COVID-19 in workers.\(^{32}\)

Remote temperature sensing devices: Several tech companies have developed temperature sensing devices using thermal imaging technology. This means that temperature readings can be measured at a distance.\(^{33}\) These devices are now being sold en masse across the globe, including by U.S. companies.\(^{34}\)

There is a wide range of temperature sensing devices--from remote surveillance cameras to devices that can attach to smartphones or smart eyeglasses.
Such temperature sensing devices could be used in checkpoint scenarios for entry into grocery stores, malls, restaurants, and in daily police street stops.

In Point 5 below, we discuss how these devices are being used in surveillance tracking to “predict” the next pandemic hot zone or outbreak.

Examples include:

- In the US, a threat detection screening company Athena Security\(^{35}\), whose system was previously used to detect guns, now offers what it calls a “Fever Detection COVID19 Screening System.” It deploys "artificially intelligent thermal cameras" to detect fevers and alert customers to the presence of someone who is suspected of carrying the coronavirus. The company is pitching the device to be used in grocery stores, hospitals and voting locations and claims that the device is being deployed at government agencies, airports and Fortune 500 companies.\(^{36}\)

- Dermalog, a biometrics company that makes fingerprint, iris and facial recognition technology, has now added a feature to determine temperature\(^{37}\) and pitched it as a new security feature to companies. The Thai government is already using Dermalog’s technology\(^{38}\) as part of its border control system.

- Biometrics technology company Tello has launched temperature-sensing systems as part of its facial recognition technology to detect individuals suspected of COVID-19. The device is designed to work even if individuals are wearing masks.\(^{39}\)

*Thermal camera system can scan body temperatures on people as quickly as they can walk through to help identify individuals potentially infected by COVID-19 or other viruses. Source: PR Newswire.*
3. INVASIVE STAY-HOME MONITORING

Electronic monitoring has been likened to digital jails. These devices generally take the form of ankle “shackles” which employ GPS tracking though companies have developed other types of tracking devices such as e-bracelets and smartphone apps. These devices allow governments and its vendors to monitor a person’s location and sometimes their blood alcohol level.

With more than 125,000 devices in use, with approximately 30,000 of them attached to immigrants on any given day, electronic monitoring is commonly used as a condition of pretrial release, probation, and release from immigration detention. Wide spread documentation exists about problems related to electronic monitoring - from causing medical distress to device failures.

Electronic monitoring compromises users’ privacy in a number of ways. It is not clear who can access that data, or what, if any, regulations apply to its storage, use, information security, and retention. One common device can even record calls and conversations without users’ consent or knowledge.

In the wake of COVID-19, governments are expanding the use of electronic monitoring to enforce health quarantines and place people under medical surveillance. Below are two use examples.

**Electronic monitoring for people under humanitarian release**

We expect local and state entities to increase their use of electronic monitoring in response to COVID-19, particularly with respect to incarcerated individuals under humanitarian release. Officials have confirmed hundreds of COVID-19 cases at local, state and federal correctional facilities, leading to hunger strikes in immigrant detention centers and demands for release and protections from the pandemic. In response to public outcry, government authorities across the country have released thousands of individuals in an effort to reduce prison crowding and slow the infection. Some governmental entities have required the use of electronic monitoring, while others have not, demonstrating that governments can release people in jail *without* increased use of surveillance.
Examples:

- Jails in Wisconsin, Kentucky, and Virginia are releasing individuals in jail through the required use of electronic monitoring.45

- New Jersey is expected to release 1000 people from its jails through a jail consent order, which allows for temporary release and the discretionary commutation of sentences.46 But the order does not require any form of electronic monitoring.

- In Massachusetts, the state’s highest court has sharply limited the use of GPS ankle bracelets to promote social distancing, as attaching a device necessarily requires close contact between government personnel and the person monitored.47

Electronic monitoring to enforce quarantines

Federal and local agencies may use electronic monitoring to enforce medical quarantines for those with or suspected of contracting COVID-19 or to enforce social distancing. Such use of electronic monitors has not occurred in the U.S. but has happened in other countries. For example, Hong Kong is requiring all incoming travelers to wear electronic wristbands and use a smartphone app to ensure they remain in isolation for a compulsory 14-day quarantine.48 In Taiwan, cell phone location data is used to create an “electronic fence” which alerts authorities when a quarantined person moves too far away from their home.49

4. WORKER MONITORING AND SURVEILLANCE

In recent years, the electronic and biometric surveillance of employees has grown rapidly across all industries, with employers monitoring employee facial expressions and tone of voice to gauge their emotional states, location and movements, and computer and social media activity.50 A 2018 survey found that 22% of organizations worldwide in various industries are using employee-movement data, 17% are monitoring work-computer-usage data, and 16% are using Microsoft Outlook- or calendar-usage data.51 Employers like Amazon and Walmart say it helps them boost productivity. But studies suggest that this employer-surveillance state can increase workplace stress, promote worker
alienation, lower job satisfaction, and convey the perception that the quantity of work one generates is more important than its quality.52

Employers are now turning their surveillance technologies to monitor employee health during the pandemic. We can expect that companies will use this crisis to expand the use of these technologies on workers. Here are examples of how workplace surveillance is or may expand.

Temperature and other biometrics checks. Temperature checks normally constitute an overly broad medical exam under the Americans with Disabilities Act (because the exam is not “job-related and consistent with business necessity”) and under various state non-discrimination laws. But an updated Equal Employment Opportunity Commission (EEOC) guidance allows employers to measure an employee’s body temperature where the state or local health authorities have found that COVID-19 is widespread in the community.53

Some businesses like Amazon and Walmart, and hospitals are already administering temperature checks on employees and more employers are expected to do so once sheltering orders lift.54 As biometrics-tracking is on the rise, employers could require employees to submit to temperature sensing devices. As discussed in Point 2, employers may use thermal cameras to detect fevers among workers once in the workplace.

Video surveillance to enforce public health guidelines and detect illness. Employers may also use more basic (but nonetheless invasive) video surveillance to monitor whether workers are complying with public health guidelines such as hand washing and social distancing or exhibiting other virus symptoms such as coughing or shortness of breath. Recently, Amazon announced that it would use video surveillance to enforce social distancing and that employees who violate
such guidelines would be terminated.\textsuperscript{55}

**Remote work surveillance.** As more workers shift to working remotely, some employers may want to ensure that worker productivity does not lapse. We may see more employers incorporating products that take regular screenshots of employees’ work, monitor keystrokes and web usage, and photograph them at their desks using computer webcams. All of this can be done remotely.\textsuperscript{56}

## 5. PREDICTIVE MODELING OF HEALTH DIAGNOSTICS

The COVID-19 pandemic is expected to be lucrative business for data analytics companies who want to create predictive tools to limit disease spread and future outbreaks.\textsuperscript{57} These companies develop intelligence and predictive analytics tools to scrape, collect, and analyze mass quantities of personal, biometric, biographic, and location data that is then sold to federal and state government agencies. Right now, they are developing technologies to: (1) predict which localities could be the next COVID-19 “hot zones” and/or (2) predict the next public health crisis or disease outbreak.

On the surface, technologies that allow public health officials to better predict where and when a health crisis could take place make good sense. Early detection could be critical to healthcare delivery and saving lives.\textsuperscript{58}

However, predictive analytics in health surveillance is new and debates over implementation are unresolved. Such predictive data analytics involve technology companies collecting and analyzing massive amounts of personal and private data with little oversight or justification of costs and benefits. For example, this predictive modeling includes analyzing the following types of sensitive health data: patient medical records and biographic data, insurance claims, medical billing codes, lab results, medications, doctor’s notes, social media, zip codes, medical bills, and reimbursement requests for medical care.

Data collected by researchers is often publicly available, but technology companies are not bound by the same principles of transparency, deep study, data quality assurances, and motivation to divulge methodology.\textsuperscript{59} Lastly, concerns are emerging whether automation and data analytics in public health spaces are further exacerbating health disparities by failing to provide resources
to communities that need it most. The reality is that the data already shows that communities with poor healthcare infrastructure will suffer disproportionately from this health crisis. Black people are disproportionately dying from this disease.

Below are some examples of how governments and companies are deploying predictive modeling of disease outbreaks:

- Lumiata AI, a predictive analytics company for patient health management, provides federal and state health agencies and hospitals predictions on the spread of the COVID-19 disease. It advertises a strategic partnership with BlueCross BlueShield and a data asset of 100 million patients including raw data on patient medical records, insurance claims, medical billing codes, and lab results.

- Created by researchers, epidemiologists and software developers at Boston Children’s Hospital, HealthMap mines news websites, government alerts, eyewitness accounts, and other data sources for outbreaks of various illnesses reported around the world. The site aggregates those cases on a global map, with outbreaks displayed in real time, in an effort to predict and track disease outbreaks.

- Companies are developing temperature and other biomedical health tracking, such as through medical devices or remote cameras, aimed at detecting the early signs of illness. See Point 2 for more information.

**RECOMMENDATIONS**

We must organize to ensure that temporary measures taken during a public health emergency are not later misused to increase deportation and criminalization. We must hold accountable the corporations that stand to profit from this massive new health care “surveillance” system and ensure that they do not create the new benchmarks for privacy protections and health surveillance.

In making these recommendations, we recall our experience with the Patriot Act and Homeland Security Act, two post 9/11 laws that were written in a few days but ended up permanently expanding surveillance and detention powers of the federal government. We must not make the same mistakes by ensuring that
emergency powers do not continue beyond this pandemic crisis. The rapidly changing nature of this pandemic and the need for life saving measures is critical, but surrendering critical privacy rights and granting more police power will have long term impacts on the rights of Black, Brown, Asian, immigrant and other marginalized communities facing criminalization and/or deportation.

1) **Strong privacy protections are needed; limit data use, collection and sharing:**

- Health care surveillance and data use should be restricted to uses related to a legitimate, proven health care purpose and time-limited to the COVID-19 pandemic. Sensitive information, such as immigration status, collected by health agencies or service providers should not be used to criminalize populations, particularly Black, Brown, and immigrant communities.

- Data sharing should be limited to federal, state, and local public health agencies engaged in fighting the spread of COVID-19 pandemic. For example, patient information should not be shared with ICE.

- States and localities must ensure that new products do not invade the privacy rights of all their residents and that health access is secured. Refer to Just Futures Law and Mijente Take Back Tech Toolkit for local communities interested in the process of researching, educating, and demanding accountability around surveillance and data collection done by their own local governments and police departments.

2) **Abstain from using and/or limit emergency powers:**

- Health agencies should abstain from invoking emergency or broad police powers. If invoked, they must sunset at the end of this crisis.
The CDC and Health and Human Services Agency must disclose to Congress, including the newly created Select House Committee on the Coronavirus Crisis and PRAC about plans to use emergency powers created in any coronavirus-related bill. Oversight should focus on ensuring privacy protections are not violated by corporations or health agencies.

3) **Limit cell phone tracking data collection:**

- Cell phone users should have clear notice and choice to opt-in to sharing their location data with cell phone surveillance companies.

- Cell phone surveillance companies should only collect and share *aggregated* location data to the lowest feasible resolution with government health agencies.\(^6^5\)

- Any claims that data is anonymous must be based on evidence and supported with sufficient information regarding how it has been anonymized. Any government agency seeking individualized data on a person’s location should be required to show probable cause and a criminal warrant.

4) **Require transparency from federal, state, local agencies and collaborating companies:**

Participating agencies and companies should be required to disclose the following:
• What data is being collected by or shared with government agencies and the motivation or use-justification for seeking the data;

• Which companies are involved in the health surveillance system? Contracts, monies, and types of data collected must be shared with the public;

• How the data is or will be used and the time-limit retention or use;

• Specify the bases for using emergency powers or national security exemptions used by government in acquiring this data;

• All data retention and auditing practices.

CONCLUSION

True community health comes from care, not invasive surveillance. The United States currently leads the world in COVID-19 infections. While countries in Asia and Europe have been able to activate existing public health and social service infrastructure, containment efforts in the United States have been seriously hindered by systemic government failures to prioritize healthcare delivery, disaster preparation, labor protections and other social safety net infrastructure.

From hospital closures to social service cuts to lack of health care coverage, America’s deep structural inequalities are exacerbating the spread of the virus—with poor, Black and Brown communities suffering the worst health outcomes before and during the pandemic.66

We strongly urge governments to invest in these forms of community safety, instead of turning to technology companies selling quick fixes and flashy solutions through untested and invasive surveillance. Heavy handed policing tactics against the most vulnerable communities are counterproductive, causing communities to retreat further into the shadows at a time when self-reporting
and seeking hospital care are critical to addressing this crisis.\textsuperscript{67}

Below are just some of the alternative, effective ways that governments could drastically mitigate the public health crisis arising from this and future pandemics:

- Expand health care coverage and fund more hospitals and community health clinics;
- Strengthen our social safety net including investing in social services, mental health, food, nutritional, and homeless services;
- Adopt decriminalization and decarceration policies for police and jails;
- Provide essential protective gear and hygiene supplies to the public free of charge;
- Expand income relief so people do not have to risk working and infection due to socio-economic status;
- Freeze rent payments and evictions in the short-term and pass affordable housing policies in the long-term;
- Support mutual aid networks and ensure that they are not criminalized by stay-at-home orders during the pandemic.

In the past few weeks, community members, advocates and policy makers across the country have demanded action and published detailed resources on each of the above categories and beyond. It is time for federal and state governments to invest in community care and services rather than fall back on criminalization and surveillance.
ADDITIONAL RESOURCES


- Immigrant Legal Resource Center, Practice Alert, Temporary Changes to USCIS in Response to COVID-19.

- National Lawyers Guild and Vision Change Win, Know Your Rights During COVID, last updated April 7th, 2020.

WRITTEN & DESIGNED BY

Paromita Shah, Julie Yihong Mao, Sejal Zota, & Ellen Kemp

WITH HELP FROM

Ana Cantu

© 2020, Just Futures Law
REFERENCES


2 The World Health Organization defines public health surveillance as the continuous, systematic collection, analysis, and interpretation of health-related data needed for the planning, implementation, and evaluation of public health practice. The CDC, which sits under the jurisdiction of the Health and Human Services Agency, serves as the primary federal agency responsible for creating policy related to mitigating and ending disease.


**Surveillance During COVID-19**


See fn. 17, referring to see e.g. COVID-19 Mobility Data Network, https://www.covid19mobility.org/#about (collaboration amongst Facebook, Camber Systems, Cuebiq, various research institutions that analyze the data and share it with localities).


Electronic monitoring is concerning on a number of levels. Typically, people on monitors must charge their devices daily and cannot leave their homes without permission. Sometimes the location trackers fail because of problems with the cellular signal, which risks a return to jail. Monitoring often leaves people in debt with user fees ranging from $3 to $35 per day. These devices have also caused a range of medical complications, from pain and bruising to electric shocks to emotional stress. See more at Ruthie Epstein, *Opinion: ICE is using an alternative to immigrant detention. But it's inhumane*, WorldPost, Washington Post, (Sep 5, 2018), [https://www.washingtonpost.com/news/theworldpost/wp/2018/09/05/trump-immigrants-2/](https://www.washingtonpost.com/news/theworldpost/wp/2018/09/05/trump-immigrants-2/).


Workers essential

require this medical information to be secured from unauthorized breach or access.

will be used (to maintain a safe work environment). Several information is being collected (body temperature) and the purpose(s) for which the information Act (CCPA) may be entitled to a prior notice, which must describe at the time of collection, what

However, in California, employees of businesses covered by the California Consumer Privacy Act (CCPA) may be entitled to a prior notice, which must describe at the time of collection, what information is being collected (body temperature) and the purpose(s) for which the information will be used (to maintain a safe work environment). Several state privacy and breach laws require this medical information to be secured from unauthorized breach or access.


Olivia Solon, Big Brother isn’t just watching: workplace surveillance can track your every move,


